livingsecurity

Leveraging Human Risk Management for Your Career Advancement

Securing a promotion in any professional field requires strategic planning, consistent effort, and effective communication of accomplishments. As someone leading Security Awareness and Training, understanding how Human Risk Management (HRM) can aid in this progression is pivotal.

There is a great article published by Ruchi Sinha, PhD, Associate Professor of Organizational Behavior at the University of South Australia Business School, featured in the Harvard Business Review, where she creates a roadmap for earning a promotion in various roles. For the purpose of this discussion, we will tailor these insights to the domain of Security Awareness and Training.

Step 1

"Planting the Seed"

Promotions rarely occur spontaneously; they require careful preparation and evidence-based advocacy. Starting a dialogue with your manager six to nine months prior to seeking a promotion is best as everyone will need time to plan. This conversation should revolve around:

- Clearly articulating the requirements for advancing to the next career level during routine one-on-one meetings.
- Identifying key performance indicators (KPIs) crucial for the role.
- Aligning your metrics with organizational objectives and presenting proactive strategies understood by the C-suite and Board
- Implementing success metrics that reflect your contribution to fostering a culture of security consciousness and reducing organizational risk, backed by insightful data analysis.
- Documenting achievements meticulously in a brag folder to substantiate your case during promotion discussions.

Closing the gap to a promotion:

At Living Security, we speak to hundreds of Security & Awareness Leaders on a monthly basis. We consistently hear that reporting (Board/C-suite and across the business) is very important, but the metrics they look for are narrowly focused and often revolve around:

- **Phishing**
  Open Rates, Click Rates, Report Rates, Credentials Harvested
- **Training**
  Completion Percentages, Engagement Rates, Blog Subscribers
- **Culture**
  Cyber Champions Program Enrollment

Although these metrics are very important, they are not the metrics and focus areas to move the business forward. To make the next jump, you need to enhance the program and that starts by measuring outcomes and not activities.

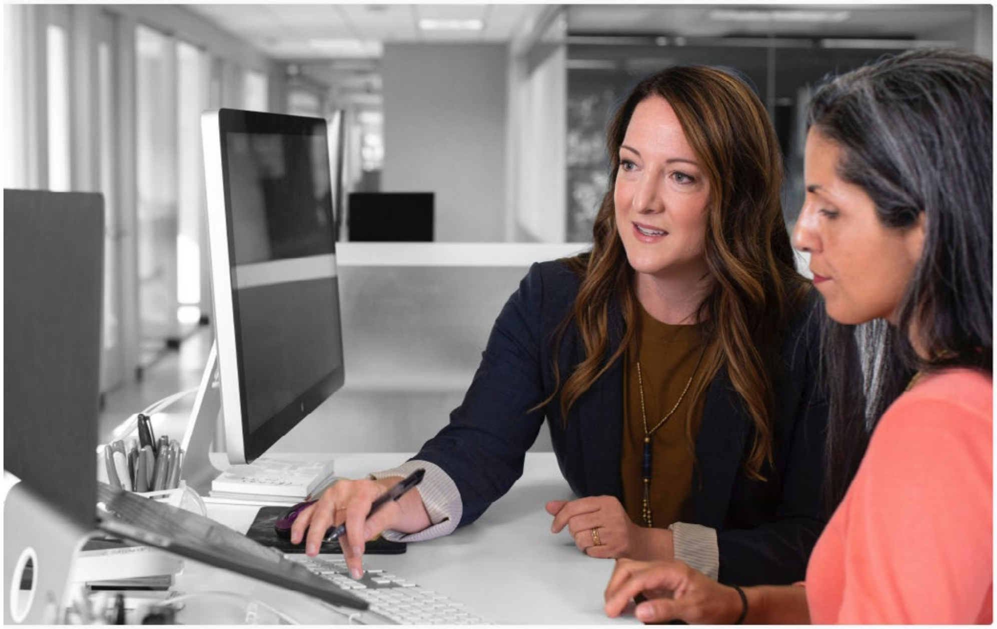
Human Risk Management Metrics Quantify the Impact of Security & Awareness Leaders

HRM programs and platforms enable SAT leaders to extend the measurement and reporting of key metrics beyond phishing, training, and culture. Risk can also be quantified by:

- Access Level: which groups or employees have elevated access to sensitive information
- Departments: which teams, departments, or office locations are at elevated risk
- Security Risks: which groups are at heightened risk of data, identity, malware, and/or social engineering threats

Example HRM Metrics to track and report to build a case for promotion

If the business is concerned about their Cyber Insurance Coverage, show them how your last campaign jumped MFA adoption by 37%, decreasing the likelihood of an incident. Show them how you have built a culture of ownership and accountability, e.g. increasing your report rate by 27%, because you communicate with your audience regularly and through a variety of channels (email, Slack, Teams, etc.). When you can tie back your value to the business objectives, you are viewed differently.



Step 2

Document your achievements in a brag folder

Now that you have a focus on larger organizational goals, the big first step is complete. Once you have achieved a major goal (defined by you and your manager), and have the data to back it up, it is time to start this conversation. To do this, you need to be able to show quantitative HRM metrics backing your value and growth within the organization.

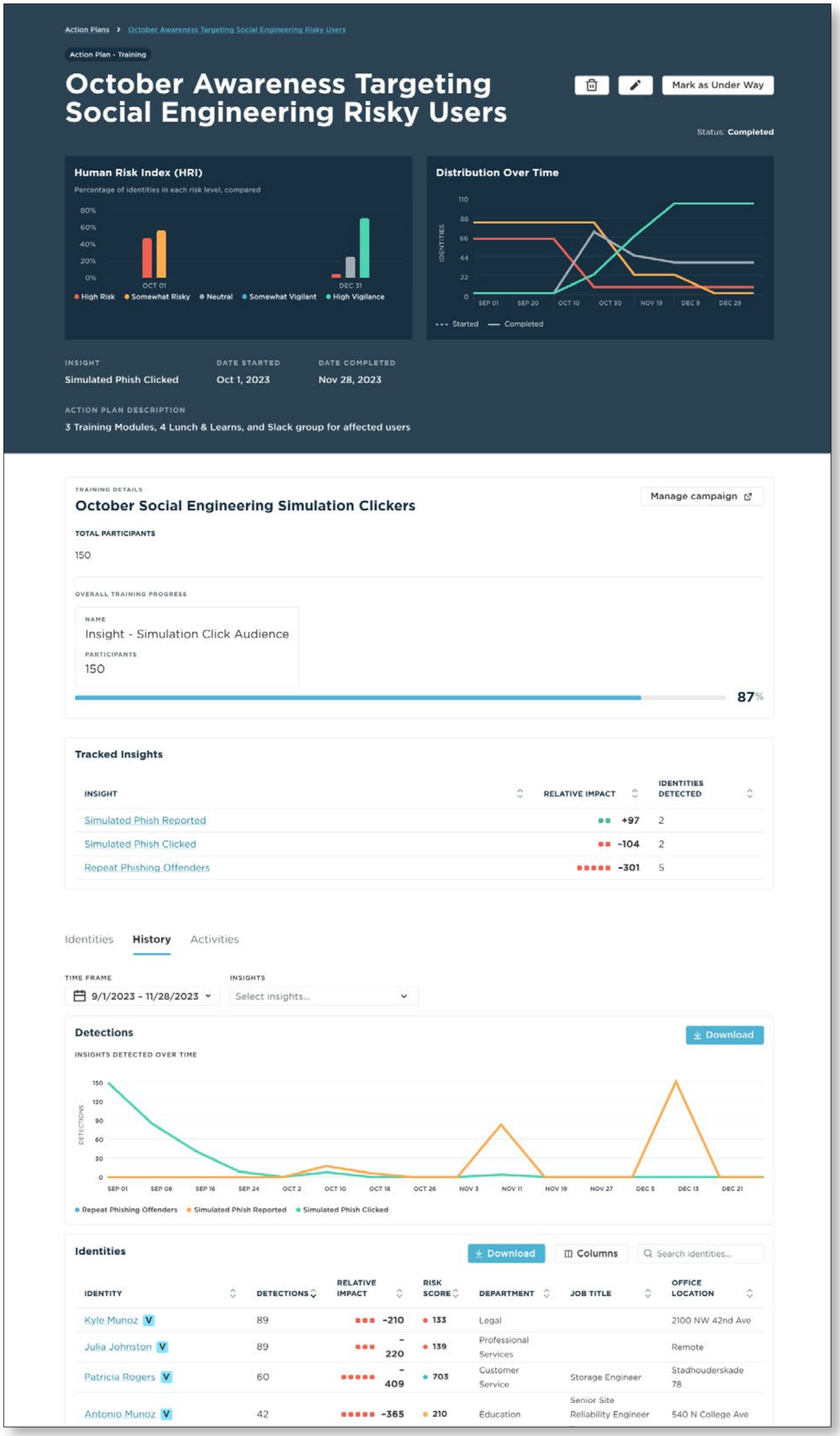
Here is an actual example from one of our customers. The client ran enterprise-wide phishing simulations in the summer months and came to the conclusion, with their CISO, that they need to focus their program efforts on a specific risk group based on three data points:

- Privileged users (IAM tool data)...
- Who have clicked on a simulated or real phish (Phishing data), and...
- Who been heavily targeted (Email Security data)

The Director of Training and Awareness came up with a proposed campaign for October with a focus on the risk cohort they identified. The program would consist of:

- A Slack Message, notifying the group of an upcoming training they will be enrolled in
- A Slack invite to one of four lunch and learn sessions that will cover two major areas:
    - The responsibility that comes with having elevated access
    - Not just how to spot a phish but the importance to the security team and company of reporting the phish.
- Enrollment into three micro learning videos, each one minute, on the topics covering privileged access and spear-phishing.

Here is the outcome of that work targeting 150 High Risk Users who fit their risk profile and the results that went straight into the “brag folder.”



Action Plans › October Awareness Targeting Social Engineering Risky Users
Action Plan - Training
Mark as Under Way

October Awareness Targeting Social Engineering Risky Users

Status: **Completed**

INSIGHT	DATE STARTED	DATE COMPLETED
Simulated Phish Clicked	Oct 1, 2023	Nov 28, 2023

ACTION PLAN DESCRIPTION

3 Training Modules, 4 Lunch & Learns, and Slack group for affected users

TRAINING DETAILS

October Social Engineering Simulation Clickers

TOTAL PARTICIPANTS

150

OVERALL TRAINING PROGRESS

NAME

Insight - Simulation Click Audience

PARTICIPANTS

150

87%

Tracked Insights

INSIGHT	RELATIVE IMPACT	IDENTITIES DETECTED
Simulated Phish Reported	🟩🟩 +97	2
Simulated Phish Clicked	🟥🟥 -104	2
Repeat Phishing Offenders	🟥🟥🟥🟥🟥 -301	5

TIME FRAME: 9/1/2023 - 11/28/2023

INSIGHTS: Select insights...

Detections

Identities

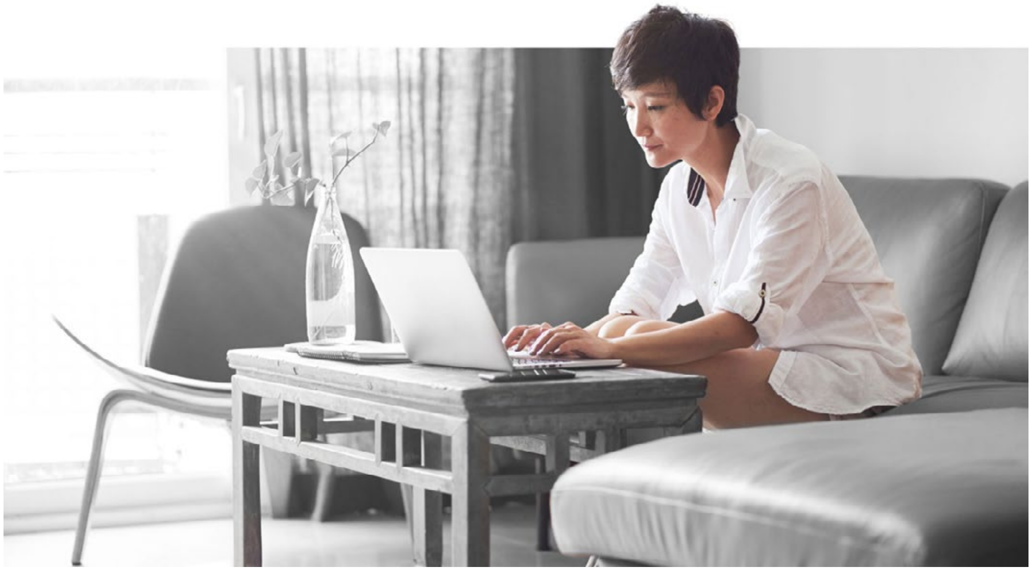
IDENTITY	DETECTIONS	RELATIVE IMPACT	RISK SCORE	DEPARTMENT	JOB TITLE	OFFICE LOCATION
Kyle Munoz V	89	🟥🟥🟥 -210	● 133	Legal		2100 NW 42nd Ave
Julia Johnston V	89	🟥🟥🟥 -220	● 139	Professional Services		Remote
Patricia Rogers V	60	🟥🟥🟥🟥🟥 -409	● 703	Customer Service	Storage Engineer	Stadhouderskade 78
Antonio Munoz V	42	🟥🟥🟥🟥🟥 -365	● 210	Education	Senior Site Reliability Engineer	540 N College Ave

- By November 28, they only had one user of the 150 repeat click
- All 150 users completed at least one of the two actions: lunch and learn or video modules
- All 150 users over the next two months REPORTED at least one suspicious email (real or simulated) - moving high risk users into the vigilant category.

The data above does two things:

- Shows that a focused training program can shift behavior
- Demonstrates a resilient culture, not based on surveys, but based on users understanding their risk, their willingness to learn in short stints, and adopting their learning into their day to day work.

Our client found a problem the CISO deeply cared about. They created a plan to drive this risk down. Then they had the metrics to prove that the efforts worked and now they have a compelling action plan to run again when new users fit this same profile in the future!



Step 3

Making the Ask

Approaching your manager for a promotion requires confidence, supported by a compelling narrative of your accomplishments aligned with organizational objectives.

Emphasize:

- Tangible outcomes of your initiatives, such as increased MFA adoption or decreased instances of sharing sensitive information.
- Your proactive approach to identifying and addressing security risks, as evidenced by higher report rates of suspicious emails post-training.
- Expressing readiness to assume greater responsibility and contribute meaningfully to organizational goals.

Sample Dialogue:

> "I believe I've consistently met our shared expectations and contributed positively to our objectives. I am eager to take on more challenges and advance in my career. I welcome your guidance on how I can further contribute to our team and the organization as a whole."

In essence, leveraging HRM practices entails strategic alignment of your achievements with organizational goals, effective communication of value propositions, and proactive engagement in career advancement discussions. By adopting this approach, security professionals can navigate their career pathways with confidence and competence.

livingsecurity

Living Security, the global leader in human risk management, transforms human risk into proactive defense by quantifying human risk to engage the human with relevant content and communications to truly change human behavior. Living Security solves the challenges of human risk through risk identification, awareness and training, and risk reduction all through an integrated platform. Living Security is trusted by security-minded organizations like MasterCard, Verizon, Biogen, AmerisourceBergen, Hewlett Packard, and more. Learn more at www.livingsecurity.com.